

20 SEPTEMBER 2002



Operations

OPERATIONS SECURITY (OPSEC) PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: 7 AF/OPSEC (Capt Michael Donahue)

Certified by: 7 AF/AA-3 (Col Ellsworth Tulberg)

Pages: 13

Distribution: F

This instruction establishes procedures for administering the Seventh Air Force (7 AF) OPSEC program. It applies to all units assigned or attached to 7 AF, including deployed and provisional units, 51st Fighter Wing (51 FW) at Osan AB, Korea and 8th Fighter Wing (8 FW) at Kunsan AB, Korea. **Attachment 1-Attachment 5** are designed to assist OPSEC Program Managers/POC's develop a stronger OPSEC program. These attachments are only examples and should be tailored to meet the needs of the organization.

1. General. All 7 AF commanders must establish a viable OPSEC program. Units should reference AFD 10-11, *Operations Security*, and AFI 10-1101, *Operations Security*, as a starting point for their OPSEC program. AFI 10-1101 does an excellent job explaining the OPSEC process and USAF OPSEC programs. Joint Pub 3-54, *Joint Doctrine for Operations Security*, provides the basis for OPSEC in a joint environment.

2. Responsibilities:

2.1. The Commander of 7 AF:

2.1.1. Delegates authority for the administration of the 7 AF OPSEC program to the 7 AF A-3 (DO).

2.1.2. Will appoint in writing a primary and alternate 7 AF OPSEC Program Manager, who will be the 7 AF OPR for OPSEC.

2.1.3. Designates the 7 AF/A39 as an office of collateral responsibility (OCR) for 7 AF OPSEC.

2.2. Wing, Group, and Group-equivalent Commanders will appoint in writing primary and alternate OPSEC program managers.

2.3. 7 AF OPSEC program managers will:

2.3.1. Review and revise 7 AF Commander's policy letter for approval.

2.3.2. Review and revise 7 AF Commander's directive letter to subordinate commanders to ensure they establish a visible OPSEC program.

2.3.3. Ensure all the following organizations have OPSEC program managers appointed:

2.3.3.1. 607 AOG.

2.3.3.2. 607 AIG.

2.3.3.3. 607 AFS.

2.3.3.4. 607 ASOG.

2.3.3.5. 607 ASG.

2.3.3.6. 51 FW.

2.3.3.7. 8 FW.

2.3.4. Review, revise as needed, and publish 7 AF Critical Information List (CIL) annually.

2.3.5. Conduct OPSEC working groups at least quarterly or more often as needed. The following OPSEC program managers are required to attend OPSEC working group meetings:

2.3.5.1. 607 AOG.

2.3.5.2. 607 AIG.

2.3.5.3. 607 AFS.

2.3.5.4. 607 ASOG.

2.3.5.5. 607 ASG.

2.3.5.6. 51 FW.

2.3.5.7. 8 FW.

2.3.6. Coordinate, plan and schedule recurring OPSEC program manager training for program managers within the Korean theater. To account for the high turnover rate of personnel in Korea, OPSEC program manager training should be offered at least semi-annually.

2.3.7. Coordinate OPSEC related assessments as required. Some examples are OPSEC Multidiscipline Vulnerability Assessment (OMDVA), Network Security Assessment (NSA) and HUMINT Vulnerability Assessment (HVA).

2.3.8. Review appropriate OPLAN's to ensure OPSEC is integrated in the entire planning process.

2.3.9. Conduct Staff Assistance Visits on 607th organizations, 51 FW and 8 FW annually. Assist other program managers with the development of their OPSEC programs as needed.

2.4. Wing, Group, and Group-equivalent Program Managers will:

2.4.1. Establish squadron level OPSEC POC's under their chain of command.

2.4.2. Ensure all units have a current CIL approved by their commanders.

2.4.3. Ensure unit OPSEC POC's are conducting their OPSEC program IAW AFI 10-1101, attachment 4.

2.4.4. Conduct Staff Assistance Visits on subordinate units as requested or required.

2.4.5. Host base level OPSEC program managers such as the 51 FW and 8 FW OPSEC program managers will liaison with OPSEC POC's at base tenant units not under any other chain of command locally, for example the 731 AMS and 5 RS.

2.5. Unit OPSEC POC's will:

2.5.1. Provide initial OPSEC training for all personnel upon assignment to include the following topics:

2.5.1.1. Purpose of OPSEC.

2.5.1.2. Role of OPSEC within Information Operations.

2.5.1.3. OPSEC process.

2.5.1.4. Foreign threat related to unit.

2.5.1.5. Critical Information for unit mission.

2.5.1.6. Job specific OPSEC indicators.

2.5.1.7. OPSEC measures to execute.

2.5.2. Conduct refresher training at least annually for individuals on extended tours.

2.5.3. Conduct an OPSEC survey at least annually.

2.5.4. Review, revise and publish unit CIL annually.

2.5.5. Conduct an OPSEC self-inspection annually.

2.5.6. Ensure unit CIL is posted near phones and unclassified computer systems.

3. Procedures:

3.1. To request Electronic Systems Security Assessment (ESSA) telecommunications monitoring support for USAF units, Commanders should send a message to PACAF/DOIO and info PACOM J-39, ACC/DOZ, AIA/DOOF, and 67 IOW/DOO. If the request is for a real world contingency or joint exercise, PACOM will put the requirement into the Joint Operations Planning and Execution System (JOPES) and the requirement gets submitted to JCS and JFCOM.

3.2. To request communications monitoring for joint units, the Joint Communications Monitoring Agency may be requested through the USFK OPSEC Program Manager. The unit OPSEC POC will submit the request to USFK J3-IO with a courtesy copy to the 7 AF OPSEC Program Manager. Prior to any equipment being hooked up for monitoring purposes (e-mail, phone, facsimile), a trusted agent will coordinate with 51 CS/SCB, PACAF NOSC, and PACAF CIO for approval.

3.3. Any questions about requesting or doing telecommunications monitoring may be directed to the ESSA personnel at the 7th Information Warfare Flight at 784-9788.

3.4. When Staff Assistance Visits are conducted the following can be expected:

3.4.1. Review content of unit OPSEC continuity book.

3.4.2. Review initial training that is provided to all newly assigned personnel.

- 3.4.3. Go through self-inspection checklist to identify shortfalls in the OPSEC program for improvement.
- 3.4.4. Discuss initiatives to increase overall OPSEC posture of the unit.
- 3.5. Procedures for developing/reviewing unit CIL
 - 3.5.1. Start with the generic Air Force CIL in [Attachment 4](#) and tailor it based on the unit mission.
 - 3.5.2. Route the initial list throughout the unit so the subject matter experts can provide inputs to the CIL.
 - 3.5.3. Prepare final CIL for Commander approval.
 - 3.5.4. Keep routing information for continuity book to show command involvement in the CIL process.

LANCE L. SMITH, Lieutenant General, USAF
Commander, Seventh Air Force

Attachment 1**EXAMPLE OPSEC SURVEY**

A1.1. OPSEC is vital to the mission here at 123 FS. In order to improve our OPSEC program, we need to determine where we can improve our efforts. Please take the time to complete this short OPSEC survey and return it to either 123 FS OPSEC POC, TSgt Jones or Capt Smith.

A1.2. Critical Information (CI) is information about friendly activities, intentions, capabilities or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary, may prevent or complicate mission accomplishment, reduce mission effectiveness, or cause loss of lives and/or damage to friendly resources. Critical information usually involves a few key elements of information concerning friendly activities or intentions that might significantly degrade mission effectiveness if revealed to an adversary. Critical information may also be derived from seemingly unrelated elements of information (indicators).

A1.3. During the past 6 months, have you heard personnel discuss critical information outside the work center? (Circle one) YES/NO.

A1.3.1. If YES, where and how often do you think this occurs?

A1.3.2. Where: _____

A1.3.3. How often (circle one): Sometimes/Often/Always.

A1.4. During the past 6 months, have you seen critical or sensitive information thrown in the trash? (Circle one) YES/NO.

A1.4.1. If YES, where and how often do you think this occurs?

A1.4.2. Where: _____

A1.4.3. How often (circle one): Sometimes/Often/Always.

A1.5. During the past 6 months, have you heard personnel discuss classified information outside the work center? (Circle one) YES/NO.

A1.5.1. If YES, where and how often do you think this occurs?

A1.5.2. Where: _____

A1.5.3. How often (circle one): Sometimes/Often/Always.

A1.6. Do personnel in your section state “phones up” and “phones down” when a non-secure phone is in use? (Circle one) YES/NO.

A1.6.1. If YES, how often do you think this occurs?

A1.6.2. How often (circle one): Sometimes/Often/Always.

A1.7. When “phones up” is stated, does discussion of critical or sensitive information cease? (Circle one) YES/NO.

A1.7.1. If YES, how often do you think this occurs?

A1.7.2. How often (circle one): Sometimes/Often/Always.

A1.8. How would you evaluate the OPSEC training you receive? (Circle one): Unsatisfactory/Marginal/Satisfactory/Excellent/Outstanding.

A1.9. How would you evaluate the squadron's OPSEC posture? (Circle one): Unsatisfactory/Marginal/Satisfactory/Excellent/Outstanding.

A1.10. How would you evaluate your personal OPSEC posture? (Circle one): Unsatisfactory/Marginal/Satisfactory/Excellent/Outstanding.

A1.11. What is your rank? () E1-E4/() E5-E9/() O1-O3/() O4-O6.

A1.12. What section do you work in? () CC/() DO/() LG/() SC/() MS.

A1.13. Where can you find a copy of the 123 FS CIL?

A1.14. What do you think would improve the squadron's OPSEC posture?

A1.15. What would you say is our biggest weakness or OPSEC concern?

THANK YOU!

PLEASE RETURN TO EITHER OPSEC POC

Attachment 2

EXAMPLE OPSEC SELF-INSPECTION

Item No.	Items	Yes	No
1	Has the commander established a program to ensure OPSEC is fully integrated into their mission?		
2	Has the commander appointed a program manager (PM) or point of contact (POC)?		
2.1	Has the OPSEC PM/POC forwarded appointment letter to higher headquarters OPSEC office of primary responsibility?		
2.2	Are visual aids identifying the OPSEC PM/POCs prominently displayed throughout the unit?		
3	Has the OPSEC PM/POC attended or requested to attend the USAF OPSEC Program Managers course?		
4	Does the OPSEC PM/POC reside in the plans or operations element of the organization?		
5	Has the OPSEC PM/POC established a continuity book?		
5.1	Are current editions of all instructions, pamphlets, directions and supplements available?		
5.2	Does the unit have local directives that define unit OPSEC program requirements, responsibilities and procedures?		
5.3	Does the continuity folder include files of past OMDVA's, surveys, SAV's and/or appraisals?		
5.4	Does the continuity book include current policy letters from unit, higher headquarters and AF?		
6	Does the OPSEC PM/POC conduct annual self-inspections?		
7	Does the OPSEC PM/POC provide risk assessments and/or recommended OPSEC measures to be implemented to senior decision makers and the commander?		
8	Does the OPSEC PM/POC review OPSEC advisory reports and ensure the commander is informed?		
7	Is OPSEC closely coordinated with the other security disciplines?		
8	Have unclassified (NIPRNET) unit web pages been reviewed for OPSEC concerns?		
9	Have OPSEC plans been developed to ensure critical information and indicators are protected?		
10	Is the unit CIL current to reflect changing circumstances and is it reviewed and approved by the commander?		

Item No.	Items	Yes	No
11	Are unit CIL's unclassified and easily accessible to unit personnel?		
12	Are contractors informed of the requirement to control and protect mission critical information?		
13	Does the OPSEC PM/POC conduct a comprehensive in-house OPSEC survey at least annually?		
14	Are unit personnel provided initial OPSEC training upon assignment and at least annually thereafter?		
15	Does the Initial OPSEC training include the purpose of OPSEC, role of OPSEC within IO, OPSEC process, foreign threat related to unit, critical information for unit mission, job specific OPSEC indicators and OPSEC measures to execute?		
16	Are OPSEC posters prominently displayed throughout the unit?		
17	Has the unit OPSEC PM/POC established and maintained liaison with the base or higher headquarters OPSEC PM?		
18	Is the OPSEC PM/POC on distribution for telecommunications monitoring or AFOSI HVA reports involving their unit?		
19	Does unit OPSEC PM/POC include provisions for reviewing plans, operations orders and exercise scenarios?		

Attachment 3

EXAMPLE UNIT OPSEC CONTINUITY BOOK TABLE OF CONTENTS

A3.1. TAB A – OPSEC MANAGER INFORMATION:

- A3.1.1. Appointment letters.
- A3.1.2. Training certificates.

A3.2. TAB B – OPSEC INFORMATION AND OVERVIEW:

- A3.2.1. Program review.
- A3.2.2. OPSEC Process.
- A3.2.3. Goals and Objectives

A3.3. TAB C – CRITICAL INFORMATION:

- A3.3.1. Unit CIL.
- A3.3.2. Higher headquarters CIL.
- A3.3.3. CIL review process and distribution.

A3.4. TAB D – POLICY AND GUIDANCE:

- A3.4.1. Commanders' policy letters.
- A3.4.2. AFPD 10-11.
- A3.4.3. AFI 10-1101.
- A3.4.4. 7 AFI 10-1101.
- A3.4.5. JP 3-54.

A3.5. TAB E – INSPECTION MATERIALS:

- A3.5.1. Unit self inspection checklist.
- A3.5.2. Most recent self inspection results.
- A3.5.3. Staff Assistance Visit results.
- A3.5.4. UCI reports and crossflow.

A3.6. TAB F – TRAINING DOCUMENTS:

- A3.6.1. Initial training.
- A3.6.2. Refresher training.
- A3.6.3. Threat assessment information.
- A3.6.4. Vulnerability assessment reports and countermeasures.

A3.7. TAB G – POC's:

- A3.7.1. MAJCOM OPSEC program managers.
- A3.7.2. USAFK/7 AF OPSEC program managers.
- A3.7.3. Wing/Group program managers.

A3.8. TAB H – MISCELLANEOUS:

- A3.8.1. Public affairs review/interaction.
- A3.8.2. Freedom of Information Act review/interaction.

Attachment 4**EXAMPLE CRITICAL INFORMATION LISTING (CIL)**

Commanders/OPSEC program managers should tailor unit CI lists to meet their needs. Please use this list as a general starting point to build an OPSEC program. The use of “USAF” as a descriptor is for example only.

A4.1. OPERATIONS: Details of or pertaining to:

- A4.1.1. Mission – nature and objectives.
- A4.1.2. Dates, times, and locations of operations or operational training.
- A4.1.3. Identity, strength, disposition, and readiness of forces.
- A4.1.4. Effect of adversary activities and operations.
- A4.1.5. IO capabilities and procedures.
- A4.1.6. Agencies/Customers requesting information or service.
- A4.1.7. Subject and results of information gathering processes.
- A4.1.8. Requests for official information to or from unit.
- A4.1.9. Operational capabilities and limitations of systems.
- A4.1.10. Vulnerabilities of U.S. and Allied systems.
- A4.1.11. Exercises and results analysis support of USAF operations or operational training.
- A4.1.12. Unit initiatives in improving technology or tactics, techniques, and procedures (TTP).
- A4.1.13. Data production and associated methods/processes, or associated strengths and weaknesses.

A4.2. PERSONNEL/LOGISTICS/ADMIN: Details of or pertaining to:

- A4.2.1. Travel by key USAF staff to or from unit.
- A4.2.2. Identification of personnel with specific offices or missions.
- A4.2.3. Association of unclassified code words with sensitive operations.
- A4.2.4. Unit strengths, shortfalls, or performance factors.
- A4.2.5. Unit training, readiness, or efficiency status.
- A4.2.6. SORTS.
- A4.2.7. Mission equipment.
- A4.2.8. Support equipment.
- A4.2.9. Personnel privacy act data.
- A4.2.10. Budget, financial, or proprietary data, especially associated with operational data.

A4.3. SECURITY: Details of or pertaining to:

- A4.3.1. Assessed vulnerabilities of the unit, physically or in information systems.
- A4.3.2. Strengths, limitations, and capabilities of unit information systems.
- A4.3.3. Configuration and architecture of systems.
- A4.3.4. Information on gaining access to unit information systems.
- A4.3.5. Current information related to why security postures have changed (FPCONS, INFOCONS, DEFCONS, etc.)

Attachment 5

POINT OF CONTACT LISTING

POC	OFFICE SYMBOL	CONTACT INFORMATION	WEB PAGE
7 AF OPSEC	7 AF/A39	DSN (315) 784-2859	https://www.osan.af.smil.mil/7afwt
PACAF OPSEC	HQ PACAF/DOIO	DSN (315) 449-7868	https://www.cidss.af.mil/doio/index.html
USFK OPSEC	USFK J3-IO	DSN (315) 723-5313	
Interagency OPSEC Support Staff	IOSS	Comm (301) 982-0323 mailto:ioss@radium.ncsc.mil	http://www.ioss.gov/
39 IOS	39 IOS/DOID	DSN (312) 579-3565	https://www.hurlburt.af.mil/milonly/tenantunits/39ios/index.htm